



日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 4月 3日

出 願 番 号

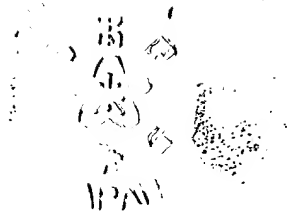
Application Number:

特願2001-104331

出 願 人

Applicant(s):

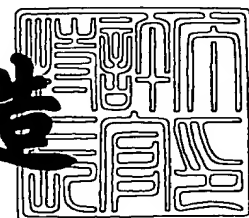
日本電信電話株式会社



2001年 6月13日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3055438

【書類名】 特許願

【整理番号】 NTTH127195

【提出日】 平成13年 4月 3日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/21  
G06F 15/62

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 重松 智志

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 斎藤 賢一

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 羽田野 孝裕

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 久良木 億

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 島村 俊重

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 町田 克之

【特許出願人】

【識別番号】 000004226

【氏名又は名称】 日本電信電話株式会社

【代理人】

【識別番号】 100064621

【弁理士】

【氏名又は名称】 山川 政樹

【電話番号】 03-3580-0961

【手数料の表示】

【予納台帳番号】 006194

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9701512

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 携帯型端末システム、生体認証装置及び携帯型端末装置

【特許請求の範囲】

【請求項 1】 携帯型端末装置と生体認証装置とからなる携帯型端末システムであって、

前記生体認証装置は、自装置を所持するユーザの生体情報を読み取る生体情報読取手段と、

予め登録された正規ユーザの生体情報とこの正規ユーザの個人情報とを記憶する第 1 の記憶手段と、

前記生体情報読取手段で読み取られた生体情報と前記第 1 の記憶手段に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、前記第 1 の記憶手段に記憶された個人情報を前記携帯型端末装置に送信する第 1 の処理装置とを有し、

前記携帯型端末装置は、前記生体認証装置から送信された個人情報を記憶する第 2 の記憶手段と、

この第 2 の記憶手段に記憶された個人情報を用いて通信処理又はデータ処理を行う第 2 の処理手段とを有することを特徴とする携帯型端末システム。

【請求項 2】 携帯型端末装置と生体認証装置とからなる携帯型端末システムであって、

前記生体認証装置は、自装置を所持するユーザの生体情報を読み取る生体情報読取手段と、

予め登録された正規ユーザの生体情報とこの正規ユーザがサービス提供を受けるのに必要なサービス情報とを記憶する第 1 の記憶手段と、

前記生体情報読取手段で読み取られた生体情報と前記第 1 の記憶手段に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、前記第 1 の記憶手段に記憶されたサービス情報を前記携帯型端末装置に送信する第 1 の処理装置とを有し、

前記携帯型端末装置は、前記生体認証装置から送信されたサービス情報を記憶する第 2 の記憶手段と、

この第 2 の記憶手段に記憶されたサービス情報を用いて通信処理又はデータ処理を行う第 2 の処理手段とを有することを特徴とする携帯型端末システム。

【請求項 3】 請求項 1 記載の携帯型端末システムにおいて、

前記個人情報、前記正規ユーザの個人識別番号を含み、

前記携帯型端末装置の第 2 の処理手段は、前記第 2 の記憶手段に前記個人情報が格納された後、この個人情報に含まれる前記個人識別番号を用いてネットワークとの回線接続を行うことを特徴とする携帯型端末システム。

【請求項 4】 請求項 2 記載の携帯型端末システムにおいて、

前記サービス情報は、ウェブサイトログインする際に使用されるパスワードを含み、

前記携帯型端末装置の第 2 の処理手段は、前記第 2 の記憶手段に前記サービス情報が格納された後、ネットワークを介してアクセスしたウェブサイトに対応するパスワードを前記サービス情報中から取得し、取得したパスワードをアクセス先のウェブサイトへ送信することを特徴とする携帯型端末システム。

【請求項 5】 自装置を所持するユーザの生体情報を読み取る生体情報読取手段と、

予め登録された正規ユーザの生体情報とこの正規ユーザの個人情報とを記憶する記憶手段と、

前記生体情報読取手段で読み取られた生体情報と前記記憶手段に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、前記記憶手段に記憶された個人情報を携帯型端末装置へ送信する処理装置とを有し、

前記個人情報を保持していない前記携帯型端末装置に前記認証結果が照合一致を示す場合のみ前記個人情報を送信することにより、前記個人情報を用いた通信処理又はデータ処理を許可することを特徴とする生体認証装置。

【請求項 6】 自装置を所持するユーザの生体情報を読み取る生体情報読取手段と、

予め登録された正規ユーザの生体情報とこの正規ユーザがサービス提供を受けるのに必要なサービス情報とを記憶する記憶手段と、

前記生体情報読取手段で読み取られた生体情報と前記記憶手段に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、前記記憶手段に記憶されたサービス情報を携帯型端末装置に送信する処理装置とを有し、

前記サービス情報を保持していない前記携帯型端末装置に前記認証結果が照合一致を示す場合のみ前記サービス情報を送信することにより、前記サービス情報を用いた通信処理又はデータ処理を許可することを特徴とする生体認証装置。

【請求項 7】 請求項 5 記載の生体認証装置において、

前記個人情報、前記携帯型端末装置とネットワークとの回線接続に必要な前記正規ユーザの個人識別番号を含むことを特徴とする生体認証装置。

【請求項 8】 請求項 6 記載の生体認証装置において、

前記サービス情報は、前記携帯型端末装置からネットワークを介してウェブサイトログインする際に使用されるパスワードを含むことを特徴とする生体認証装置。

【請求項 9】 ユーザの生体情報を用いて本人認証を行い、認証結果が照合一致を示す場合のみ正規ユーザの個人情報を送信する生体認証装置から、前記個人情報を受信して記憶する記憶手段と、

この記憶手段に記憶された個人情報をを用いて通信処理又はデータ処理を行う処理手段とを有し、

前記生体認証装置に記憶された前記個人情報を受信した場合のみ、前記個人情報をを用いた通信処理又はデータ処理を行うことを特徴とする携帯型端末装置。

【請求項 10】 ユーザの生体情報を用いて本人認証を行い、認証結果が照合一致を示す場合のみ正規ユーザがサービス提供を受けるのに必要なサービス情報を送信する生体認証装置から、前記サービス情報を受信して記憶する記憶手段と、

この記憶手段に記憶されたサービス情報をを用いて通信処理又はデータ処理を行う処理手段とを有し、

前記生体認証装置に記憶された前記サービス情報を受信した場合のみ、前記サービス情報をを用いた通信処理又はデータ処理を行うことを特徴とする携帯型端末

装置。

【請求項 1 1】 請求項 9 記載の携帯型端末装置において、  
前記個人情報、前記正規ユーザの個人識別番号を含み、  
前記携帯型端末装置の処理手段は、前記記憶手段に前記個人情報が格納された後、この個人情報に含まれる前記個人識別番号を用いてネットワークとの回線接続を行うことを特徴とする携帯型端末装置。

【請求項 1 2】 請求項 1 0 記載の携帯型端末装置において、  
前記サービス情報は、ウェブサイトログインする際に使用されるパスワードを含み、  
前記携帯型端末装置の処理手段は、前記記憶手段に前記サービス情報が格納された後、ネットワークを介してアクセスしたウェブサイトに対応するパスワードを前記サービス情報中から取得し、取得したパスワードをアクセス先のウェブサイトへ送信することを特徴とする携帯型端末装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、ユーザの生体情報を用いて本人認証を行う例えば携帯電話機等の携帯型端末システム、生体認証装置及び携帯型端末装置に関するものである。

【0 0 0 2】

【従来の技術】

従来より、携帯電話機等の携帯型端末装置には、電話番号、電子メールアドレス等の個人情報が保存されている。このような個人情報が正規のユーザ以外の第三者に漏洩するのを防ぐため、個人情報へのデータアクセス処理にパスワードを設定して、第三者が個人情報に不正にアクセスすることを防止していた。

また、近年、携帯型端末装置からネットワークを介してウェブサイトへアクセスし、例えば商品購入などの電子商取引を行うことが可能となった。このような電子商取引においても、ユーザの正当性確認のためにパスワードが用いられている。

【0 0 0 3】

## 【発明が解決しようとする課題】

しかしながら、従来の携帯型端末装置では、正規ユーザ以外の第三者がデータアクセスに必要なパスワードを不正に取得すると、携帯型端末装置に記憶された個人情報にアクセスすることが可能となるため、個人情報が漏洩する可能性があった。

同様に、正規ユーザ以外の第三者がサービス情報、例えば電子商取引に必要なパスワードを不正に取得すると、第三者は正規ユーザになりすまして電子商取引を行うことが可能となるため、携帯型端末装置が不正に使用されて正規ユーザに課金がなされるといった問題が起こる可能性があった。

本発明は、上記課題を解決するためになされたもので、個人情報及びサービス情報の漏洩と不正な電子商取引とを防止することができる携帯型端末システム、生体認証装置及び携帯型端末装置を提供することを目的とする。

## 【0004】

## 【課題を解決するための手段】

本発明の携帯型端末システムは、携帯型端末装置（１）と生体認証装置（２）とからなり、前記生体認証装置は、自装置を所持するユーザの生体情報を読み取る生体情報読取手段（２２）と、予め登録された正規ユーザの生体情報とこの正規ユーザの個人情報とを記憶する第１の記憶手段（２３）と、前記生体情報読取手段で読み取られた生体情報と前記第１の記憶手段に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、前記第１の記憶手段に記憶された個人情報を前記携帯型端末装置に送信する第１の処理装置（２４）とを有し、前記携帯型端末装置は、前記生体認証装置から送信された個人情報を記憶する第２の記憶手段（１５）と、この第２の記憶手段に記憶された個人情報を用いて通信処理又はデータ処理を行う第２の処理手段（１４）とを有するものである。

また、本発明の携帯型端末システムは、携帯型端末装置と生体認証装置とからなり、前記生体認証装置は、自装置を所持するユーザの生体情報を読み取る生体情報読取手段と、予め登録された正規ユーザの生体情報とこの正規ユーザがサービス提供を受けるのに必要なサービス情報とを記憶する第１の記憶手段と、前記



生体情報読取手段で読み取られた生体情報と前記第 1 の記憶手段に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、前記第 1 の記憶手段に記憶されたサービス情報を前記携帯型端末装置に送信する第 1 の処理装置とを有し、前記携帯型端末装置は、前記生体認証装置から送信されたサービス情報を記憶する第 2 の記憶手段と、この第 2 の記憶手段に記憶されたサービス情報を用いて通信処理又はデータ処理を行う第 2 の処理手段とを有するものである。

また、本発明の携帯型端末システムの 1 構成例において、前記個人情報とは、前記正規ユーザの個人識別番号を含み、前記携帯型端末装置の第 2 の処理手段は、前記第 2 の記憶手段に前記個人情報が格納された後、この個人情報に含まれる前記個人識別番号を用いてネットワークとの回線接続を行うものである。

また、本発明の携帯型端末システムの 1 構成例において、前記サービス情報は、ウェブサイトログインの際に使用されるパスワードを含み、前記携帯型端末装置の第 2 の処理手段は、前記第 2 の記憶手段に前記サービス情報が格納された後、ネットワークを介してアクセスしたウェブサイトに対応するパスワードを前記サービス情報中から取得し、取得したパスワードをアクセス先のウェブサイトへ送信するものである。

#### 【 0 0 0 5 】

また、本発明の生体認証装置は、自装置を所持するユーザの生体情報を読み取る生体情報読取手段と、予め登録された正規ユーザの生体情報とこの正規ユーザの個人情報とを記憶する記憶手段と、前記生体情報読取手段で読み取られた生体情報と前記記憶手段に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、前記記憶手段に記憶された個人情報を携帯型端末装置に送信する処理装置とを有し、前記個人情報を保持していない前記携帯型端末装置に前記認証結果が照合一致を示す場合のみ前記個人情報を送信することにより、前記個人情報を用いた通信処理又はデータ処理を許可するものである。

また、本発明の生体認証装置は、自装置を所持するユーザの生体情報を読み取る生体情報読取手段と、予め登録された正規ユーザの生体情報とこの正規ユーザ

がサービス提供を受けるのに必要なサービス情報とを記憶する記憶手段と、前記生体情報読取手段で読み取られた生体情報と前記記憶手段に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、前記記憶手段に記憶されたサービス情報を携帯型端末装置に送信する処理装置とを有し、前記サービス情報を保持していない前記携帯型端末装置に前記認証結果が照合一致を示す場合のみ前記サービス情報を送信することにより、前記サービス情報を用いた通信処理又はデータ処理を許可するものである。

また、本発明の生体認証装置の 1 構成例において、前記個人情報、前記携帯型端末装置とネットワークとの回線接続に必要な前記正規ユーザの個人識別番号を含むものである。

また、本発明の生体認証装置の 1 構成例において、前記サービス情報は、前記携帯型端末装置からネットワークを介してウェブサイトログインする際に使用されるパスワードを含むものである。

#### 【 0 0 0 6 】

また、本発明の携帯型端末装置は、ユーザの生体情報を用いて本人認証を行い、認証結果が照合一致を示す場合のみ正規ユーザの個人情報を送信する生体認証装置から、前記個人情報を受信して記憶する記憶手段と、この記憶手段に記憶された個人情報を用いて通信処理又はデータ処理を行う処理手段とを有し、前記生体認証装置に記憶された前記個人情報を受信した場合のみ、前記個人情報を用いた通信処理又はデータ処理を行うものである。

また、本発明の携帯型端末装置は、ユーザの生体情報を用いて本人認証を行い、認証結果が照合一致を示す場合のみ正規ユーザがサービス提供を受けるのに必要なサービス情報を送信する生体認証装置から、前記サービス情報を受信して記憶する記憶手段と、この記憶手段に記憶されたサービス情報を用いて通信処理又はデータ処理を行う処理手段とを有し、前記生体認証装置に記憶された前記サービス情報を受信した場合のみ、前記サービス情報を用いた通信処理又はデータ処理を行うものである。

また、本発明の携帯型端末装置の 1 構成例において、前記個人情報は、前記正規ユーザの個人識別番号を含み、前記携帯型端末装置の処理手段は、前記記憶手

段に前記個人情報が格納された後、この個人情報に含まれる前記個人識別番号を用いてネットワークとの回線接続を行うものである。

また、本発明の携帯型端末装置の 1 構成例において、前記サービス情報は、ウェブサイトログインの際に使用されるパスワードを含み、前記携帯型端末装置の処理手段は、前記記憶手段に前記サービス情報が格納された後、ネットワークを介してアクセスしたウェブサイトに対応するパスワードを前記サービス情報中から取得し、取得したパスワードをアクセス先のウェブサイトへ送信するものである。

【 0 0 0 7 】

【発明の実施の形態】

〔実施の形態の 1〕

以下、本発明の実施の形態について図面を参照して詳細に説明する。図 1 は本発明の第 1 の実施の形態となる携帯型端末システムの外觀図である。図 1 ( a ) に示すように、携帯型端末システムは、システムの本体である携帯型端末装置 1 と、生体認証装置 2 とから構成される。携帯型端末装置 1 には、生体認証装置 2 を差し込むためのスロットが設けられており、このスロットに生体認証装置 2 を差し込んで携帯型端末装置 1 と生体認証装置 2 とを接続し、生体認証装置 2 により本人認証が行われると携帯型端末装置 1 にアクセスできるようになっている（図 1 ( b ) ）。

【 0 0 0 8 】

図 2 は携帯型端末装置 1 の構成を示すブロック図である。携帯型端末装置 1 は、生体認証装置 2 との接続のために前記スロットに配設された外部端子 1 0 と、生体認証装置 2 とのインタフェースとなるインタフェース装置 1 1 と、例えば基地局等との間で電波の送受信を行うアンテナ 1 2 と、アンテナ 1 2 を介して音声、画像又はテキスト等のデータの送受信を行う通信手段である無線送受信装置 1 3 と、端末装置全体を制御し、送受信データを処理する処理装置 1 4 と、情報記憶のための記憶装置 1 5 と、複数のキースイッチからなる入力装置 1 6 と、画面表示を行う液晶パネル等からなる表示装置 1 7 と、ユーザの音声をマイクロホンで集音して音声データに変換する音声入力装置 1 8 と、受信された音声データを

アナログ音声信号に変換してスピーカから出力する音声出力装置 19 とを有している。

#### 【0009】

図 3 (a) は生体認証装置 2 の斜視図、図 3 (b) は生体認証装置 2 の構成を示すブロック図である。生体認証装置 2 は、携帯型端末装置 1 との接続のための外部端子 20 と、携帯型端末装置 1 とのインタフェースとなるインタフェース装置 21 と、ユーザの生体情報を読み取る生体情報読取手段となるセンサ 22 と、予め登録された正規ユーザの生体情報とこの正規ユーザの個人情報及びサービス情報とを記憶する記憶装置 23 と、センサ 22 で読み取った生体情報と記憶装置 23 に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、記憶装置 23 に記憶された個人情報及びサービス情報を携帯型端末装置 1 に送信する処理装置 24 とを有している。生体認証装置 2 は、外部端子 20 以外の全ての機能が 1 つの L S I チップに搭載されている形でもよいし、その他の構成でもよい。

#### 【0010】

以下、本実施の形態の携帯型端末システムの動作を図 4 を用いて説明する。ここでは、ユーザの生体情報として指紋を用いるものとして説明する。まず、携帯型端末装置 1 を使って電話をかけようとするユーザは、自身が所持する生体認証装置 2 を携帯型端末装置 1 のスロットに差し込む（図 4 ステップ 101）。これにより、携帯型端末装置 1 と生体認証装置 2 とが外部端子 10, 20 を介して接続される。

#### 【0011】

生体認証装置 2 の記憶装置 23 には、正規ユーザの指紋画像データと、この正規ユーザの個人識別番号、氏名、住所、生年月日及びクレジットカード番号等の個人情報と、電話帳のデータ、電子メールアドレス帳のデータ及びパスワード等のサービス情報とが予め記憶されている。個人識別番号は、通信事業者が正規ユーザに付与した識別番号であり、例えば正規ユーザの電話番号である。携帯型端末装置 1 の記憶装置 15 には、通信処理やデータ処理等の携帯型端末装置 1 の動作に必要なプログラムが格納されているが、前記個人情報及びサービス情報は格

納されていない。

【 0 0 1 2 】

次に、ユーザは、生体認証装置 2 による本人認証を受けるべく、センサ 2 2 上に指を載せる（ステップ 1 0 2）。センサ 2 2 は、ユーザの指紋画像を読み取る（ステップ 1 0 3）。処理装置 2 4 は、センサ 2 2 によって読み取られた指紋画像と記憶装置 2 3 に予め登録された正規ユーザの指紋画像とを照合して本人認証を行う（ステップ 1 0 4）。処理装置 2 4 における認証アルゴリズムには様々な方式があり、センサ 2 2 で読み取った指紋画像の特徴点を抽出して正規ユーザの指紋画像の特徴点と比較する特徴点抽出方式や、センサ 2 2 で読み取った指紋画像を正規ユーザの指紋画像と直接比較するパターンマッチング方式などがある。

【 0 0 1 3 】

処理装置 2 4 は、指紋画像が一致し、認証結果が OK である場合（ステップ 1 0 5 において YES）、生体認証装置 2 を所持するユーザを正規ユーザと判断して、このユーザによる携帯型端末装置 1 へのアクセスを許可する。すなわち、処理装置 2 4 は、個人識別番号等の個人情報と、電話帳のデータ、電子メールアドレス帳のデータ及びパスワード等のサービス情報とを記憶装置 2 3 から読み出し、読み出した個人情報及びサービス情報をインタフェース装置 2 1 を介して携帯型端末装置 1 に送出する（ステップ 1 0 6）。また、処理装置 2 4 は、指紋画像が一致せず、認証結果が NG である場合、生体認証装置 2 を所持するユーザが正規ユーザではない判断して、携帯型端末装置 1 への個人情報及びサービス情報の送出を拒否する（ステップ 1 0 7）。

【 0 0 1 4 】

次に、携帯型端末装置 1 の処理装置 1 4 は、生体認証装置 2 から送られた個人情報及びサービス情報をインタフェース装置 1 1 を介して受信し記憶装置 1 5 に格納する（ステップ 1 0 8）。記憶装置 1 5 に個人情報及びサービス情報が格納されることにより、携帯型端末装置 1 を使用することが可能になる（ステップ 1 0 9）。

【 0 0 1 5 】

ステップ 1 0 9 において、例えばユーザが入力装置 1 6 を操作して電話帳のデ

ータから着信先の電話番号を選択し、入力装置16の発信ボタンを押下すると、処理装置14は、記憶装置15に記憶された個人識別番号と選択された着信先電話番号とを無線送受信装置13に出力する。無線送受信装置13は、個人識別番号と着信先電話番号とを無線信号に変換してアンテナ12に出力し、アンテナ12は、無線信号をネットワーク（移動網の基地局）に送出する。

## 【0016】

携帯型端末装置1からの発呼に応じて、基地局は、受信した無線信号に含まれる着信先電話番号を基に着信先の電話機を呼び出し、着信先の電話機が応答すると、携帯型端末装置1と着信先の電話番号とを回線接続する。着信先の電話機からの音声は、アンテナ12で受信された無線信号が無線送受信装置13で復調され、復調された音声データが音声出力装置19でアナログ音声信号に変換されて音声出力装置19のスピーカから出力されることにより、再生される。

## 【0017】

一方、携帯型端末装置1のユーザの音声は、音声入力装置18のマイクロホンで集音されて音声入力装置18で音声データに変換され、無線送受信装置13で無線信号に変換されてアンテナ12から送信される。以上で、携帯型端末装置1を携帯電話機として使用することが可能になる。

## 【0018】

また、ステップ109において、ユーザが入力装置16を操作して電子メールを作成し、電子メールアドレス帳から着信先の電子メールアドレスを選択して、入力装置16の発信ボタンを押下すると、携帯型端末装置1の処理装置14は、記憶装置15に記憶された個人識別番号と所定の着信先電話番号（例えばメールサービスに割り当てられた番号）とを上記音声通信の場合と同様にネットワークに送出する。

## 【0019】

ネットワークを介してメールサーバと回線接続された後、処理装置14は、記憶装置15に記憶されたユーザの電子メールアドレスと、選択された着信先の電子メールアドレスと、作成された電子メールの内容とを含むデータをネットワークに送出する。一方、電子メールの受信の場合には、アンテナ12で受信された

無線信号が無線送受信装置 1 3 で復調され、復調されたデータが処理装置 1 4 で文字データに変換されることにより、受信した電子メールの内容が記憶装置 1 5 に格納され、表示装置 1 7 の画面に表示される。以上で、携帯型端末装置 1 を携帯型メール端末装置として使用することが可能になる。

## 【 0 0 2 0 】

また、携帯型端末装置 1 を画像通信の可能な端末装置として使用する場合、処理装置 1 4 は、記憶装置 1 5 に格納された画像データをネットワークに送出する。一方、画像データの受信の場合には、アンテナ 1 2 で受信された無線信号が無線送受信装置 1 3 で復調されることにより、復調された画像データが記憶装置 1 5 に格納され、表示装置 1 7 の画面に表示される。

## 【 0 0 2 1 】

また、電源オンやデータアクセス等の処理に予めパスワードが設定されている場合、処理装置 1 4 は、パスワードが設定されている処理の実行をユーザから要求されたとき、パスワードの入力を要求するメッセージを表示装置 1 7 に表示させる。そして、処理装置 1 4 は、ユーザが入力装置 1 6 を操作して入力したパスワードと記憶装置 1 5 のサービス情報に含まれるパスワードとを照合して、パスワードが一致する場合のみ、要求された処理を実行する。これにより、ユーザは、携帯型端末装置 1 の電源オンや、個人情報又はサービス情報の閲覧・編集等の処理を行うことができる。編集した個人情報又はサービス情報を生体認証装置 2 に送って、生体認証装置 2 に記憶された個人情報又はサービス情報を更新することも可能である。

## 【 0 0 2 2 】

携帯型端末装置 1 の使用後、ユーザは、入力装置 1 6 の電源ボタンを押下して携帯型端末装置 1 の電源をオフにする（ステップ 1 1 0）。この電源オフに応じて、表示装置 1 7 等への電力供給が停止される。電源ボタンがオフにされても処理装置 1 4 への電力供給は継続されており、処理装置 1 4 は、電源オフに応じて、記憶装置 1 5 に記憶されている個人情報及びサービス情報を消去する（ステップ 1 1 1）。個人情報及びサービス情報を消去するのは、携帯型端末装置 1 に個人情報及びサービス情報が残らないようにするためである。そして、ユーザは、

携帯型端末装置 1 のスロットから生体認証装置 2 を引き抜く（ステップ 1 1 2）

。

【 0 0 2 3 】

以上のように、本実施の形態では、個人情報及びサービス情報が生体認証装置 2 に格納されており、指紋による本人認証の結果が OK の場合のみ、携帯型端末装置 1 に個人情報及びサービス情報が送付される。このため、正規ユーザ以外の第三者がパスワードを不正に取得したとしても、指紋による本人認証の段階で携帯型端末装置 1 への個人情報及びサービス情報の送付が拒否されるので、第三者は、携帯型端末装置 1 から個人情報及びサービス情報を不正に取得することはできない。したがって、パスワードの不正取得による個人情報及びサービス情報への不正アクセスを防止することができ、セキュリティを向上させることができる。

。

【 0 0 2 4 】

また、本実施の形態では、個人識別番号（電話番号）が生体認証装置 2 に格納されており、指紋による本人認証の結果が OK の場合のみ、携帯型端末装置 1 に個人識別番号が送付されて付与される。このため、ユーザは、複数の携帯型端末装置 1 を 1 つの個人識別番号で使用することができ、ユーザにとっての利便性を向上させることができる。

【 0 0 2 5 】

また、正規ユーザ以外の第三者が正規ユーザの携帯型端末装置 1 と生体認証装置 2 とを不正に取得したとしても、指紋による本人認証の段階で携帯型端末装置 1 への個人識別番号送付が拒否されるので、第三者は、携帯型端末装置 1 を使用することができない。したがって、セキュリティを向上させることができ、携帯型端末装置 1 が不正に使用されて正規ユーザに課金となされるといった問題を防ぐことができる。

【 0 0 2 6 】

また、本実施の形態では、1 つの生体認証装置 2 を複数の携帯型端末装置 1 に差し替えて使うことができる。このため、ユーザは、個人情報及びサービス情報の管理・編集を生体認証装置 2 に対してのみ行えばよいので、ユーザにとっての



利便性とセキュリティとを向上させることができる。

【0027】

なお、本実施の形態では、携帯型端末装置1の使用開始時に本人認証を行い、本人認証がOKの場合に、全ての個人情報及びサービス情報を生体認証装置2から携帯型端末装置1に送出するようにしているが、携帯型端末装置1の使用中有ある個人情報又はサービス情報（例えば電話帳のデータ）が必要になったときに生体認証装置2による本人認証を行って、認証結果がOKの場合、必要とされる個人情報又はサービス情報を生体認証装置2から携帯型端末装置1に送出するようにしてもよい。

【0028】

また、携帯型端末装置1の使用開始時に本人認証を行い、本人認証がOKの場合に、個人識別番号だけを生体認証装置2から携帯型端末装置1に送出するようにしてもよい。個人識別番号以外の個人情報又はサービス情報については、始めから携帯型端末装置1に記憶させておいてもよいし、前述のように必要に応じて生体認証装置2から携帯型端末装置1に送ってもよい。

【0029】

〔実施の形態の2〕

図5は本発明の第2の実施の形態となる携帯型端末システムの動作を示すフローチャート図である。本実施の形態においても携帯型端末システムの構成は実施の形態の1と同様であるので、図1～図3の符号を用いて説明する。

【0030】

生体認証装置2の記憶装置23には、正規ユーザの指紋画像データが記憶されると共に、電子商取引のウェブサイト（以下、電子商店と呼ぶ）との間で予め取り決められたユーザの正当性確認のためのパスワードがサービス情報として記憶されている。その他の個人情報（例えば、正規ユーザの個人識別番号）やサービス情報（例えば、電話帳のデータ、電子メールアドレス帳のデータ、電源オンや個人情報にアクセスする際に必要となるパスワード等）については、携帯型端末装置1の記憶装置15に記憶されている。

【0031】

ユーザは、携帯型端末装置 1 を操作して、実施の形態の 1 と同様の通信処理によりインターネットに接続し、ウェブページのブラウジングを行って所望の電子商店（ウェブサーバ）にアクセスする（ステップ 2 0 1）。これにより、表示装置 1 7 の画面に電子商店のウェブページが表示される。続いて、ユーザは、表示されたウェブページを見て、ウェブページに掲載された商品の購入を決定すると、入力装置 1 6 を操作してウェブページ上で商品の購入を告知する（ステップ 2 0 2）。

## 【 0 0 3 2 】

電子商店の機能を提供する、アクセス先のウェブサーバは、携帯型端末装置 1 から商品の購入申し込みがあると、正規ユーザとの間で予め取り決めたパスワードの入力をユーザに要求する（ステップ 2 0 3）。ユーザは、ウェブページに表示されたパスワードの入力要求を見て、自身が所持する生体認証装置 2 を携帯型端末装置 1 のスロットに差し込み（ステップ 2 0 4）、生体認証装置 2 のセンサ 2 2 上に指を載せる（ステップ 2 0 5）。

## 【 0 0 3 3 】

センサ 2 2 は、ユーザの指紋画像を読み取り（ステップ 2 0 6）、処理装置 2 4 は、センサ 2 2 によって読み取られた指紋画像と記憶装置 2 3 に予め登録された正規ユーザの指紋画像とを照合して本人認証を行い、認証結果を携帯型端末装置 1 に送出する（ステップ 2 0 7）。

## 【 0 0 3 4 】

携帯型端末装置 1 の処理装置 1 4 は、生体認証装置 2 から送られた認証結果が OK である場合（ステップ 2 0 8 において YES）、アクセス中の電子商店の識別情報（電子商店の名称又は番号）を生体認証装置 2 に送出する（ステップ 2 0 9）。処理装置 1 4 は、生体認証装置 2 から送られた認証結果が NG である場合、生体認証装置 2 への電子商店識別情報の送出を拒否する（ステップ 2 1 0）。

## 【 0 0 3 5 】

生体認証装置 2 の処理装置 2 4 は、認証結果が OK で、かつ携帯型端末装置 1 から電子商店識別情報を受信した場合、この電子商店識別情報に対応するパスワードを記憶装置 2 3 から読み出し、読み出したパスワードを携帯型端末装置 1 に

送出する（ステップ 2 1 1）。携帯型端末装置 1 の処理装置 1 4 は、生体認証装置 2 から送られたパスワードをインターネットに送出する（ステップ 2 1 2）。

## 【 0 0 3 6 】

アクセス先のウェブサーバは、携帯型端末装置 1 から送られたパスワードと予め登録された正規ユーザのパスワードとを照合してユーザの正当性を確認し、パスワードが一致すれば、商品の購入を申し込んだユーザを正規ユーザと判断して、このユーザの購入申し込みを受理し、購入申し込みを受理したことをアクセス元の携帯型端末装置 1 に通知する（ステップ 2 1 3）。ユーザは、商品の購入申し込みが受理されたことを確認した上で、携帯型端末装置 1 のスロットから生体認証装置 2 を引き抜く（ステップ 2 1 4）。

## 【 0 0 3 7 】

なお、生体認証装置 2 から送られたパスワードが携帯型端末装置 1 の記憶装置 1 5 に残る可能性があるので、パスワードの使用後、実施の形態の 1 と同様にパスワードを消去することが望ましい。

## 【 0 0 3 8 】

以上のように本実施の形態では、電子商店にログインする際に使用されるパスワードが生体認証装置 2 に格納されており、指紋による本人認証の結果が OK の場合のみ、携帯型端末装置 1 にパスワードが送出されて、携帯型端末装置 1 から電子商店にパスワードが送出される。正規ユーザ以外の第三者が携帯型端末装置 1 を操作したとしても、指紋による本人認証の段階で携帯型端末装置 1 へのパスワード送出が拒否されるので、第三者は、正規ユーザになりすまして電子商取引を行うことはできない。したがって、セキュリティを向上させることができる。

## 【 0 0 3 9 】

なお、本実施の形態では、認証結果が OK の場合のみ、携帯型端末装置 1 から生体認証装置 2 に電子商店識別情報を送信するようにしているが、認証結果に関係なく電子商店識別情報を生体認証装置 2 に送信して、認証結果が OK の場合のみ、電子商店識別情報に対応するパスワードを生体認証装置 2 から携帯型端末装置 1 に送信するようにしてもよい。また、本実施の形態では、本人認証後に生体認証装置 2 から送出されるサービス情報をパスワードのみとしたが、パスワード

と共にクレジットカード番号やその他の個人情報が生体認証装置 2 から送出されるようにしてもよい。

#### 【0040】

##### [実施の形態の 3]

図 6 は生体認証装置 2 内のセンサ 22 の検出素子の概略的な断面を示す図である。センサ 22 の検出素子は、例えばシリコンからなる半導体基板 711 上の下層絶縁膜 712 上に形成された層間絶縁膜 714 上に、たとえば  $80\mu\text{m}$  角の複数のセンサ電極 715 と、格子状のアース電極 716 とを備え、複数のセンサ電極 715 とアース電極 716 とを、層間絶縁膜 714 表面で規定される同一平面上に配置している。

#### 【0041】

センサ電極 715 は、層間絶縁膜 714 上に形成されたパシベーション膜 717 で覆い、 $150\mu\text{m}$  間隔に複数個を備えるようにするとともに、Au から構成し、膜厚  $1\mu\text{m}$  程度に形成している。パシベーション膜 717 の膜厚は  $3\mu\text{m}$  程度としたので、センサ電極 715 上には、パシベーション膜 717 が約 2 ( $=3-1$ )  $\mu\text{m}$  存在している。このパシベーション膜 717 は、例えばポリイミドなどの比誘電率が 4.0 程度の絶縁物から構成される。上記下層絶縁膜 712 上には、センサ電極 715 にスルーホールを介して接続する配線 713 を形成する。この配線 713 により後段の回路と接続される。

#### 【0042】

次に、センサ 22 について更に詳しく説明する。図 7 はセンサ 22 の回路図である。図 7 において、Cf は図 6 におけるセンサ電極 715 と指 811 の皮膚との間に形成される静電容量である。容量 Cf を形成するセンサ電極 715 は Nch MOS トランジスタ Q3a のドレイン端子に接続されており、このトランジスタ Q3a のソース端子は電流 I の電流源 821 の入力側に接続されている。また、センサ電極 715 とトランジスタ Q3a との節点 N1a には、Nch MOS トランジスタ (第 1 の素子) Q2a のソース端子が接続されている。このトランジスタ Q2a のドレイン端子には、ソース端子に電源電圧 VDD が印加された Pch MOS トランジスタ (第 1 のスイッチ手段) Q1a のドレイン端子と、ドレイン端子に

電源電圧  $V_{DD}$  が印加されソース端子が抵抗  $R_a$  を介して接地に接続された NchMOS トランジスタ  $Q_{4a}$  のゲート端子とが接続されている。このトランジスタ  $Q_{4a}$  のソース端子にインバータゲート 841 が接続されている。

## 【0043】

各トランジスタ  $Q_{1a}$ ,  $Q_{3a}$  のゲート端子にはそれぞれ信号  $PRE$  (バー),  $RE$  が印加される。また、トランジスタ  $Q_{2a}$  のゲート端子には定電圧源からバイアス電圧  $V_G$  が印加される。ここで、トランジスタ  $Q_{2a}$  が非導通状態になるゲート-ソース間のしきい値電圧を  $V_{th}$  とすると、 $V_{DD} > V_G - V_{th}$  となるように電圧  $V_{DD}$ ,  $V_G$  が設定される。また、節点  $N_{1a}$ ,  $N_{2a}$  はそれぞれ寄生容量  $C_{p1a}$ ,  $C_{p2a}$  を有している。

## 【0044】

容量  $C_f$  により検出素子 810 が構成され、電流源 821 とトランジスタ  $Q_{3a}$  とにより信号発生回路 820 が構成され、トランジスタ  $Q_{1a}$ ,  $Q_{2a}$  により信号増幅回路 830 が構成され、トランジスタ  $Q_{4a}$  と抵抗  $R_a$  とインバータゲート 841 とにより出力回路 840 が構成される。出力回路 840 は、処理装置 24 と接続される。

## 【0045】

図 8 は、図 7 に示したセンサ 22 の動作を説明するためのタイミングチャートであり、図 8 (a) はトランジスタ  $Q_{1a}$  を制御する信号  $PRE$  (バー) の電位変化を示し、図 8 (b) はトランジスタ  $Q_{3a}$  を制御する信号  $RE$  の電位変化を示し、図 8 (c) は節点  $N_{1a}$ ,  $N_{2a}$  それぞれの電位変化を示している。最初、トランジスタ  $Q_{1a}$  のゲート端子には High レベル ( $V_{DD}$ ) の信号  $PRE$  (バー) が与えられ、トランジスタ  $Q_{3a}$  のゲート端子には Low レベル ( $GND$ ) の信号  $RE$  が与えられている。したがって、このときトランジスタ  $Q_{1a}$ ,  $Q_{3a}$  はともに導通していない。

## 【0046】

この状態で信号  $PRE$  (バー) が High レベルから Low レベルに変化すると、トランジスタ  $Q_{1a}$  が導通状態になる。このときトランジスタ  $Q_{3a}$  は非導通状態のままであり、信号発生回路 820 は停止状態にあるから、節点  $N_{2a}$  の

電位がVDDにプリチャージされる。また、トランジスタQ2aのゲートソース間電圧がしきい値電圧 $V_{th}$ に達してトランジスタQ2aが非導通状態になるまで、節点N1aが充電される。これにより、節点N1aの電位が $V_G - V_{th}$ にプリチャージされる。

【0047】

プリチャージが終了した後、信号PRE（バー）がHighレベルに変化すると、トランジスタQ1aが非導通状態になる。これと同時に信号REがHighレベルに変化すると、トランジスタQ3aが導通状態になり、信号発生回路820が動作状態に変化する。そして、電流源821により節点N1aに充電された電荷が引き抜かれ、節点N1aの電位がわずかに低下すると、トランジスタQ2aのゲートソース間電圧がしきい値電圧 $V_{th}$ より大きくなり、トランジスタQ2aが導通状態に変化する。これにより節点N2aの電荷も引き抜かれ、節点N2aの電位低下が開始する。

【0048】

信号REをHighレベルにする期間を $\Delta t$ とすると、 $\Delta t$ 経過後の節点N1aの電位低下 $\Delta V$ は $V_{DD} - (V_G - V_{th}) + I \Delta t / (C_f + C_{p1a})$ になる。ここで、寄生容量 $C_{p2a}$ は寄生容量 $C_{p1a}$ に対して十分小さいとしている。

【0049】

電流源821の電流 $I$ と期間 $\Delta t$ と寄生容量 $C_{p1a}$ 、 $C_{p2a}$ は、各々一定であるから、電位低下 $\Delta V$ は、センサ電極715と検出対象である指の表面811との間に発生する容量の値 $C_f$ によって決定される。この容量値 $C_f$ は、センサ電極715と指の表面811との距離によって決まるので、指紋の凹凸によって異なる。このことから、低下電位 $\Delta V$ の大きさが、指紋の凹凸を反映して変化する。この電位低下 $\Delta V$ が、入力信号として出力回路840に供給されるので、出力回路840で $\Delta V$ が入力され、指紋の凹凸を反映した信号が出力される。こうした出力回路840の出力信号が処理装置24により処理され、前述の指紋画像データとして生成される。

【0050】

なお、実施の形態の 1, 2 では、図 4、図 5 を用いて動作例を説明してきたが、動作の順序を変更しても全体の動作に矛盾をきたさない場合は、動作の順序を変更してもよい。また、実施の形態の 1, 2 では、携帯型端末装置 1 をネットワークとの通信手段を有するものとしているが、携帯可能なスタンドアロンのコンピュータとしてもよい。この場合にも、正規ユーザ以外の第三者による個人情報やサービス情報への不正アクセスを防止することができる。また、実施の形態の 1, 2 では、携帯型端末装置 1 とネットワークとの間の通信を無線通信としているが、有線通信でもよい。また、携帯型端末装置 1 と生体認証装置 2 との間の通信を有線通信としているが、無線通信でもよい。

## 【 0 0 5 1 】

また、実施の形態の 1 ~ 3 では、生体情報として指紋を用いる場合を例に挙げて説明しているが、他の生体情報としては、例えばユーザの声紋、虹彩、筆跡、手形、指の長さ、人相などがある。生体情報としてユーザの手形又は指の長さを用いる場合、生体認証装置 2 のセンサ 2 2 は、ユーザの掌又は指の画像を取り込み、処理装置 2 4 は、取り込んだ画像データを記憶装置 2 3 に予め登録された正規ユーザの掌又は指の画像データと照合する。

## 【 0 0 5 2 】

また、生体情報としてユーザの声紋、すなわちサウンドスペクトログラムを用いる場合、生体認証装置 2 のセンサ 2 2 は、ユーザの音声を集音して声紋を抽出し、処理装置 2 4 は、抽出した声紋のデータを記憶装置 2 3 に予め登録された正規ユーザの声紋データと照合する。生体情報としてユーザの筆跡を用いる場合、生体認証装置 2 のセンサ 2 2 は、ユーザのペン軌跡を取り込み、処理装置 2 4 は、取り込んだ筆跡の画像データを記憶装置 2 3 に予め登録された正規ユーザの筆跡データと照合する。

## 【 0 0 5 3 】

また、生体情報としてユーザの虹彩を用いる場合、生体認証装置 2 のセンサ 2 2 は、ユーザの虹彩を撮影し、処理装置 2 4 は、撮影した虹彩の画像データを記憶装置 2 3 に予め登録された正規ユーザの虹彩の画像データと照合する。生体情報としてユーザの人相を用いる場合、生体認証装置 2 のセンサ 2 2 は、ユーザの

顔を撮影して顔の特徴を抽出し、処理装置 2 4 は、抽出した特徴データを記憶装置 2 3 に予め登録された正規ユーザの特徴データと照合する。

【 0 0 5 4 】

【発明の効果】

本発明によれば、個人情報が生体認証装置に格納され、生体情報による本人認証の結果が OK の場合のみ、携帯型端末装置に個人情報が出送される。このため、正規ユーザ以外の第三者がパスワードを不正に取得したとしても、生体情報による本人認証の段階で携帯型端末装置への個人情報出送が拒否されるので、第三者は、携帯型端末装置から個人情報を不正に取得することはできない。したがって、パスワードの不正取得による個人情報への不正アクセスを防止することができ、セキュリティを向上させることができる。また、1 つの生体認証装置を複数の携帯型端末装置に使うことができるので、ユーザは、個人情報の管理・編集を生体認証装置に対してのみ行えばよく、ユーザにとっての利便性とセキュリティとを向上させることができる。

【 0 0 5 5 】

また、サービス情報が生体認証装置に格納され、生体情報による本人認証の結果が OK の場合のみ、携帯型端末装置にサービス情報が出送される。このため、正規ユーザ以外の第三者がパスワードを不正に取得したとしても、生体情報による本人認証の段階で携帯型端末装置へのサービス情報出送が拒否されるので、第三者は、携帯型端末装置からサービス情報を不正に取得することはできない。したがって、パスワードの不正取得によるサービス情報への不正アクセスを防止することができ、セキュリティを向上させることができる。また、1 つの生体認証装置を複数の携帯型端末装置に使うことができるので、ユーザは、サービス情報の管理・編集を生体認証装置に対してのみ行えばよく、ユーザにとっての利便性とセキュリティとを向上させることができる。また、第三者は、正規ユーザになりすましてサービス提供を受けることができなくなるので、セキュリティを向上させることができる。

【 0 0 5 6 】

また、本実施の形態では、個人識別番号が生体認証装置に格納されており、生



体情報による本人認証の結果がOKの場合のみ、携帯型端末装置に個人識別番号が送出されて付与される。このため、ユーザは、複数の携帯型端末装置を1つの個人識別番号で使用することができ、ユーザにとっての利便性を向上させることができる。また、正規ユーザ以外の第三者が正規ユーザの携帯型端末装置と生体認証装置とを不正に取得したとしても、生体情報による本人認証の段階で携帯型端末装置への個人識別番号送出が拒否されるので、第三者は、携帯型端末装置を使用することができない。したがって、セキュリティを向上させることができ、携帯型端末装置が不正に使用されて正規ユーザに課金がなされるといった問題を防ぐことができる。

【0057】

また、ウェブサイトログインの際に使用されるパスワードが生体認証装置に格納されており、生体情報による本人認証の結果がOKの場合のみ、携帯型端末装置にパスワードが送出されて、携帯型端末装置からウェブサイトへパスワードが送出される。正規ユーザ以外の第三者が携帯型端末装置を操作したとしても、生体情報による本人認証の段階で携帯型端末装置へのパスワード送出が拒否されるので、第三者は、正規ユーザになりすまして電子商取引を行うことはできない。したがって、セキュリティを向上させることができる。

【図面の簡単な説明】

【図1】 本発明の第1の実施の形態となる携帯型端末システムの外観図である。

【図2】 本発明の第1の実施の形態における携帯型端末装置の構成を示すブロック図である。

【図3】 本発明の第1の実施の形態における生体認証装置の斜視図及びブロック図である。

【図4】 本発明の第1の実施の形態となる携帯型端末システムの動作を示すフローチャート図である。

【図5】 本発明の第2の実施の形態となる携帯型端末システムの動作を示すフローチャート図である。

【図6】 生体認証装置内のセンサの検出素子の概略的な断面を示す図であ

る。

【図 7】 図 6 のセンサの回路図である。

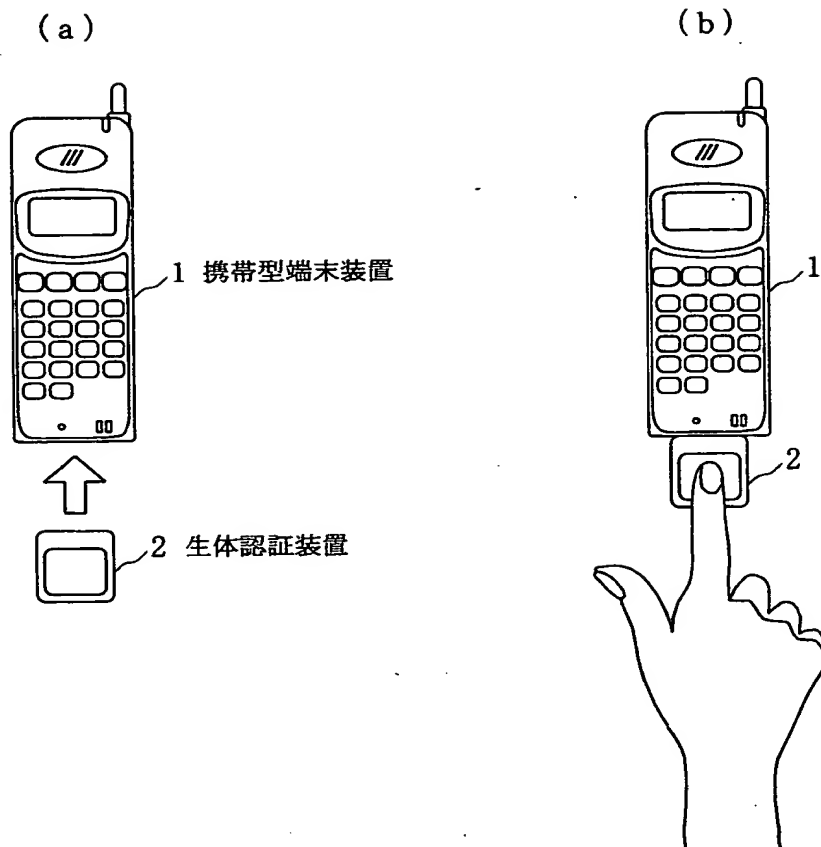
【図 8】 図 7 に示したセンサの動作を説明するためのタイミングチャートである。

【符号の説明】

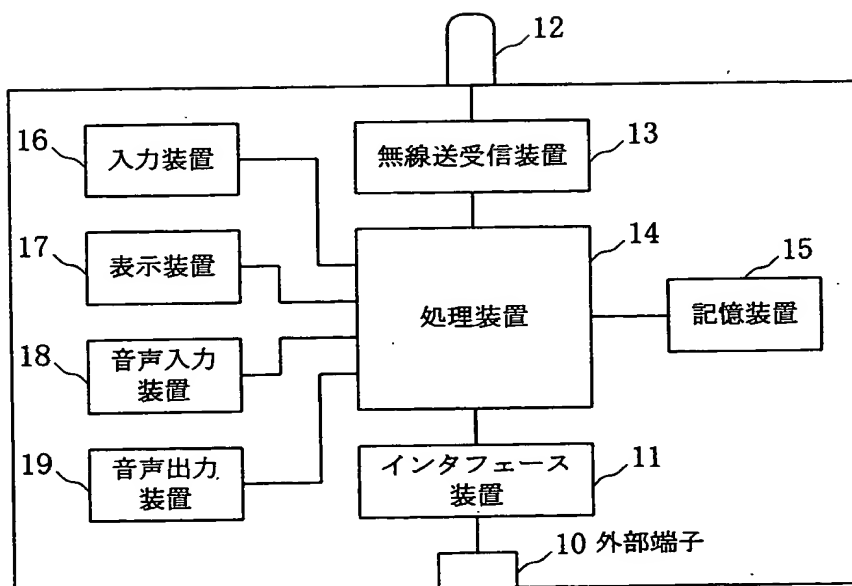
1 … 携帯型端末装置、2 … 生体認証装置、10、20 … 外部端子、11、21 … インタフェース装置、12 … アンテナ、13 … 無線送受信装置、14、24 … 処理装置、15、23 … 記憶装置、16 … 入力装置、17 … 表示装置、18 … 音声入力装置、19 … 音声出力装置、22 … センサ。

【書類名】 図面

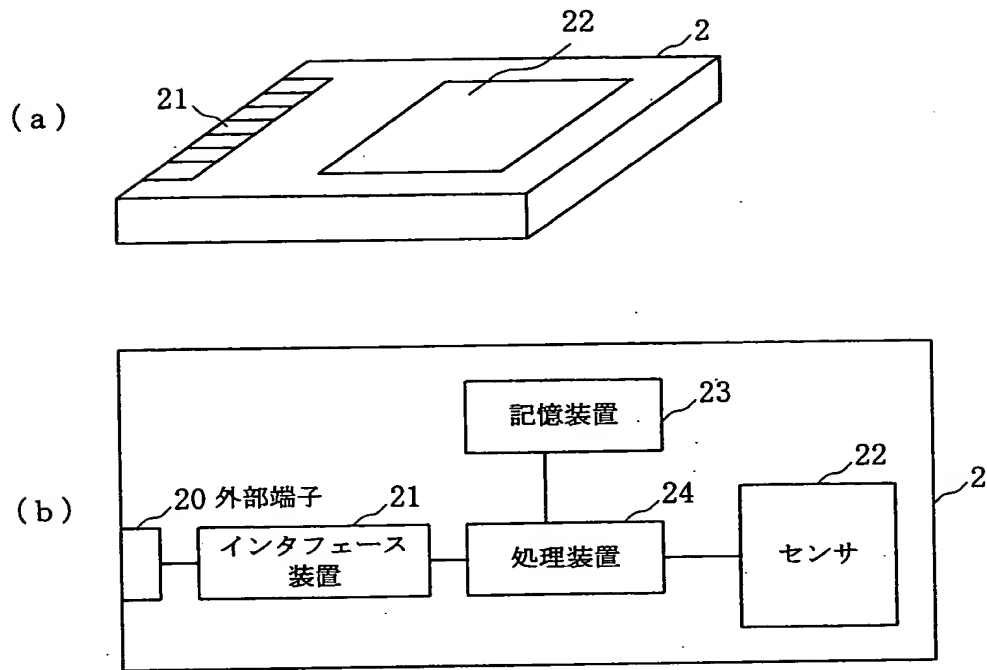
【図 1】



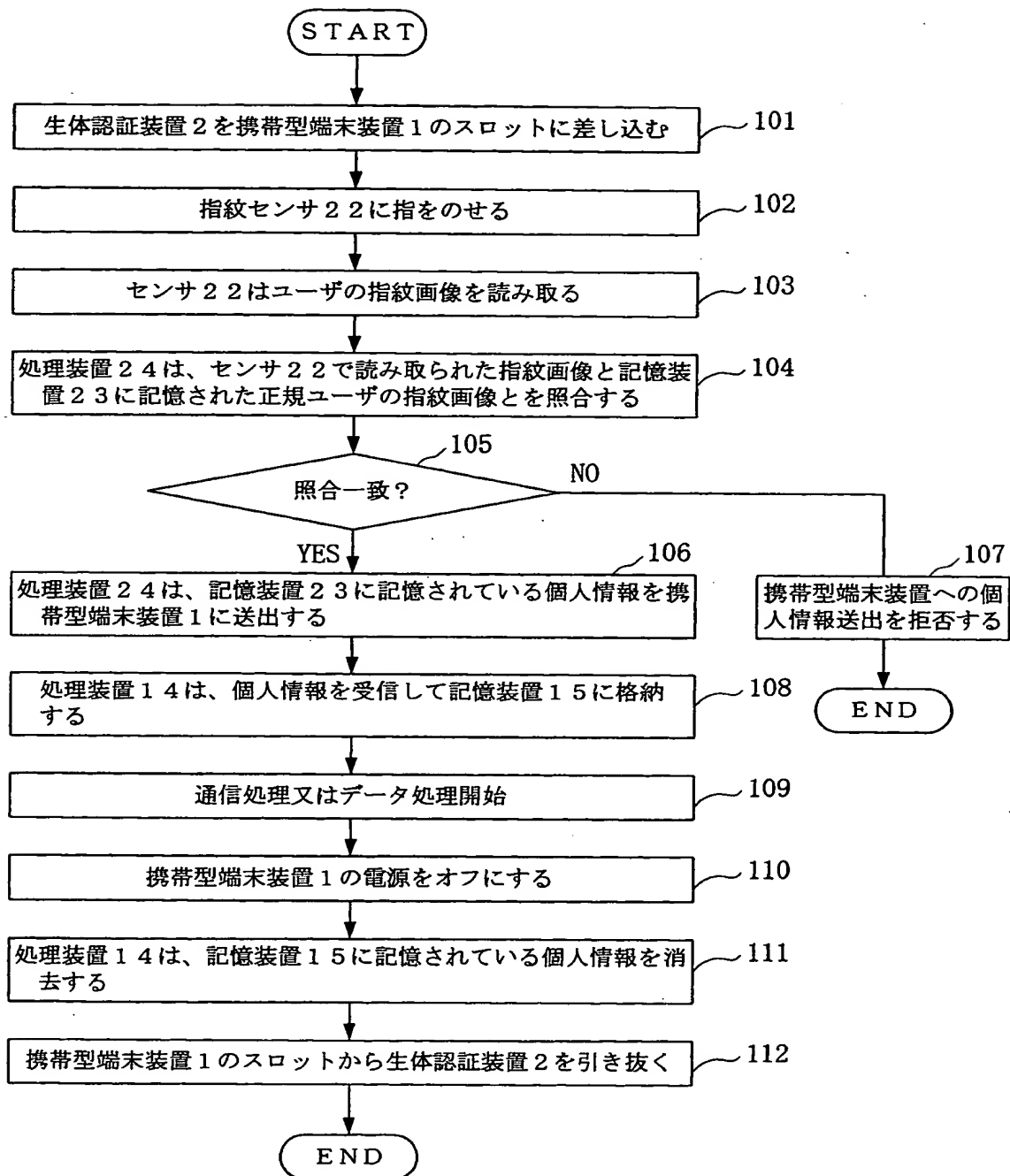
【図 2】



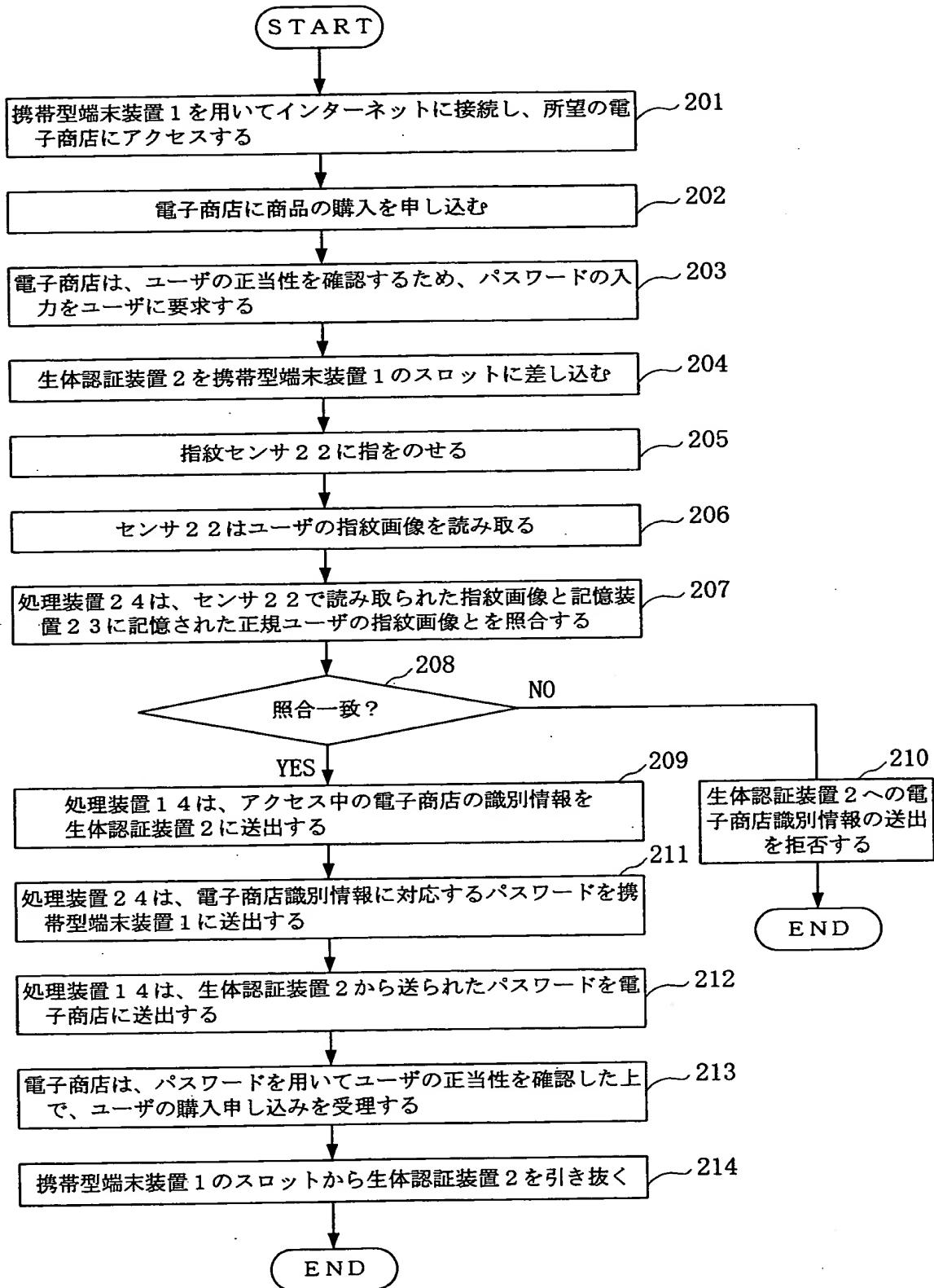
【図3】



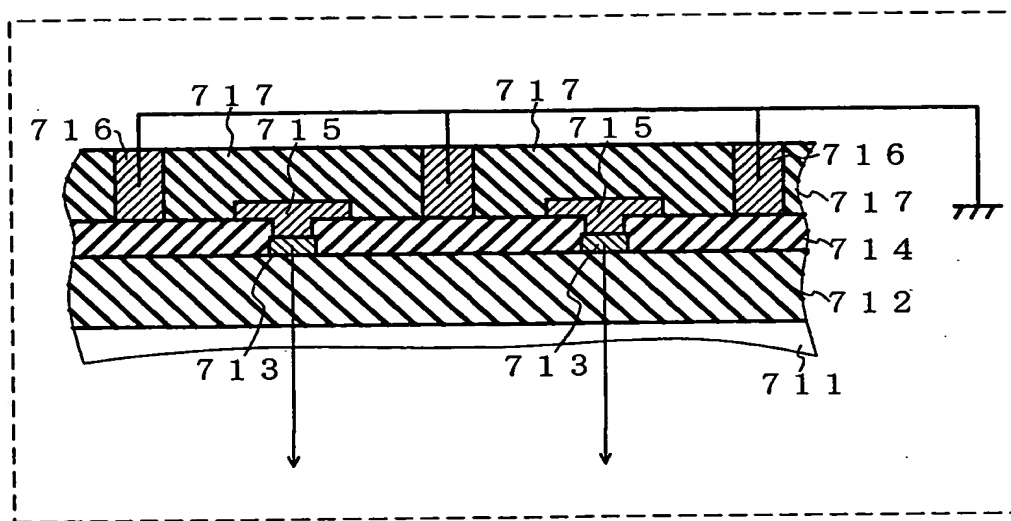
【図 4】



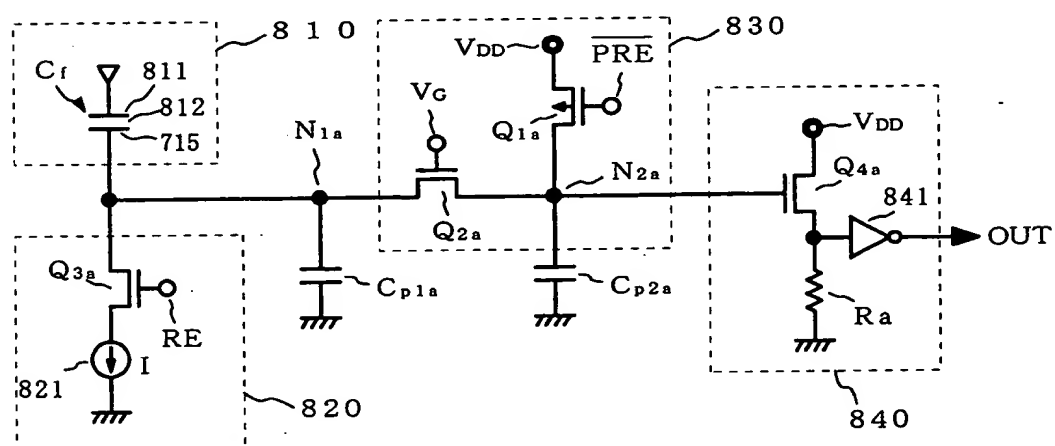
【図 5】



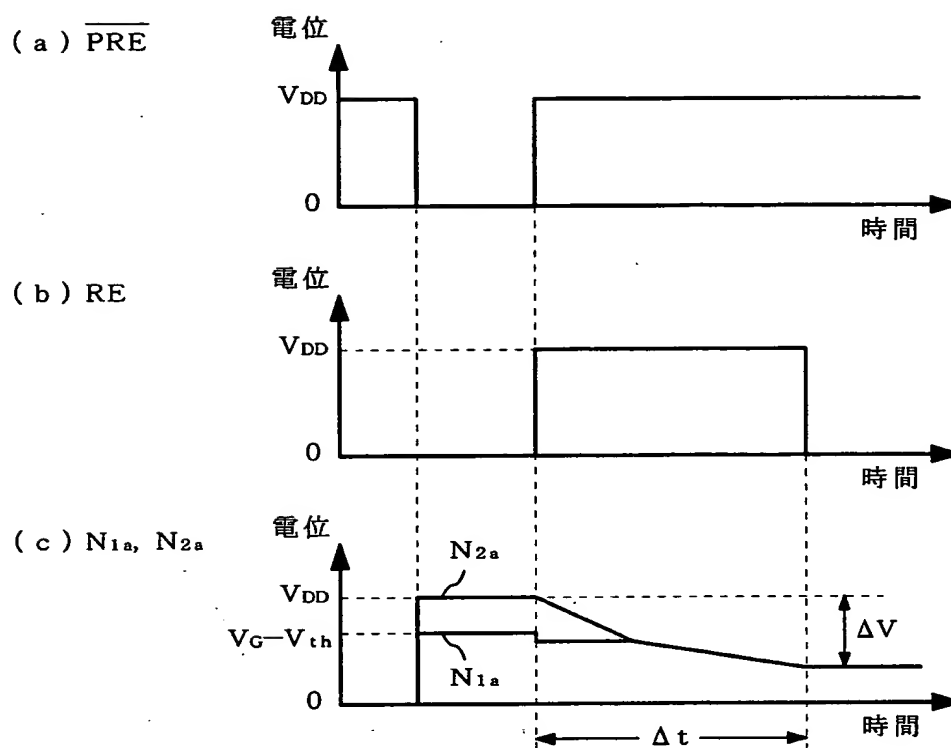
【図 6】



【図 7】



【図 8】





【書類名】            要約書

【要約】

【課題】    個人情報の漏洩と不正な電子商取引とを防止する。

【解決手段】    生体認証装置 2 は、ユーザの生体情報を読み取る生体情報読取手段と、予め登録された正規ユーザの生体情報とこの正規ユーザの個人情報とを記憶する第 1 の記憶手段と、生体情報読取手段で読み取られた生体情報と第 1 の記憶手段に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、第 1 の記憶手段に記憶された個人情報を携帯型端末装置に送信する第 1 の処理装置とを有する。携帯型端末装置 1 は、送信された個人情報を記憶する第 2 の記憶手段と、第 2 の記憶手段に記憶された個人情報を用いて通信処理又はデータ処理を行う第 2 の処理手段とを有する。

【選択図】            図 1

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 4 2 2 6 ]

1. 変更年月日	1 9 9 9 年 7 月 1 5 日
[変更理由]	住所変更
住 所	東京都千代田区大手町二丁目 3 番 1 号
氏 名	日本電信電話株式会社